REMARKS/ARGUMENTS

Claims 1-37 are pending. Claims 1, 5, 10, 15, and 20 are amended. In the Office Action, the Examiner rejected claims 1-27 under 35 USC §101 as being directed to non-statutory subject matter, rejected claims 1-9, 20-24, 28-29, 32-34, and 37 under 35 USC §103(a) as being unpatentable over Shoup et al.("Securing Threshold Cryptosystems against Chosen Ciphertext Attack") (hereinafter "Shoup"), further in view of Schneier ("Applied Cryptography"), and rejected claims 10-19, 30-31, and 35-36 under 35 USC §103(a) as being unpatentable over Shoup further in view of Schneier and U.S. Patent No. 5,991,399 to Graunke et al. (hereinafter "Graunke").

35 USC §101 Rejection

Claims 1-27 stand rejected under 35 USC §101 as being directed to non-statutory subject matter. This rejection is respectfully traversed and reconsideration is respectfully requested. With a view to early allowance of those claims, Applicant submits amendments to claim 1 and other claims to more clearly point out the concrete, useful and tangible result and that the amended claims are allowable under §101.

35 USC §103 Rejection, Shoup et al in view of Schneier

Claims 1-9, 20-24, 28-29, 32-34, and 37 stand rejected under 35 USC §103(a) as being unpatentable over Shoup in view of Schneier.

I. Claims 1-4, 28, 33

Claim 1 is allowable over Shoup and Schneier, alone or in combination, as those references fail to disclose or suggest all the elements of claim 1. For example, Claim 1 recites a "*method performed by a custodian to share a secret S among n secret owners ... comprising ... distributing n secret owner pieces to each of the n secret owners, wherein each of the secret owner pieces includes* S^d *and one of the numbers* q_1 *through* q_n." In the Office Action, the Examiner asserted that Shoup (at page 5) disclosed generating keys, encrypting a secret and distributing the secret to the owners and asserted that Schneier disclosed a key generation and encryption technique being multiple-key public-key cryptography (page 527), where the Ks are

the claimed d and the q_1 through q_n, and deleting this information after distribution (citing to Schneier, pages 184-185).

On page 5, Shoup does describe sending a public key PK and a private key SK_i to a given server P_i. Interpreting this part of Shoup in view of Schneier (page 468), one would distribute two K_i and N to each server, which is not related to the claimed steps including distributing S^d and one q_i. As explained in the specification, distributing S^d and one q_i has advantages, such as better preventing compromising the secret, e.g., by disk attack. By not distributing the public key in an easily accessible form, such as d, but rather as S^d, some attacks might be prevented. Also, by not distributing the full public key, i.e., not distributing N, other attacks might be prevented.

In addition to those elements not found in the references or their combination, claim 1 has been amended to further clarify a distinction in that the claimed method is performed by a custodian. Note that in Shoup, important calculations are required to be done by each server P_i in order to generate a decryption share σ_i.

Additionally, Shoup teaches away from combining the RSA encryption scheme of Schneier, so there is some issue as to whether the references can even be combined. On page 5, Shoup describes that each server P_i generates a share σ_i and those shares are then combined using the recovery algorithm to obtain the cleartext. In the RSA method, the result of one calculation is used for the next calculation in a serial fashion, and thus the step of parallel calculation of the shares σ_i would prohibit the use of the RSA scheme.

Furthermore, claim 1 is not obvious over Schneier's multiple-key public-key cryptography of his section 23.1 in view of Schneier's secret-sharing algorithms of section 23.2. First, all of the secret sharing algorithms of 23.2 involve solving a linear set of equations, unlike the RSA scheme. Secondly, there is no motivation to combine the RSA method, as the cited references do not suggest any benefit. By contrast, with the claimed invention, all of the secret owner pieces do not have to be received before computing a result and thus the secret owner pieces need not reside on the hard drive where they are vulnerable. This is not true of methods that solve linear systems, since all values must be available before computing.

For at least the reasons stated above, Applicants submit that claim 1 is allowable over the cited references. As claim 1 is allowable, claims 2-4 dependent therefrom are also allowable for at least that reason.

Claims 28 and 33 recite similar features as recited for claim 1, and thus claims 28 and 33 should be allowable for at least similar reasons as claim 1.

II. Claims 5-9, 29, 34

Claim 5 recites similar features as recited for claim 1, and thus claim 5 and its dependent claims 6-9 should be allowable for at least similar reasons as claim 1.

Claim 5 is allowable for additional reasons. For example, claim 5 recites "*choosing n+1 random numbers* q_1 *through* q_n *and d' that are relatively prime to M; determining a number d such that a product of* q_1 *through* q_n*, d', and d mod M equals one.*" The variable *d'* does not exist in Shoup or Schneier. Regarding Shoup, that element is not anticipated by Shoup's use of a public key, which encrypts a message, or a private key that is sent to the servers (secret owners). As for Schneier, *d'* does not correspond to any of the K_i in Schneier, since the signers have and use all of the keys not used to encrypt the message. For at least this reason, Applicants submit that claim 5 and its dependent claims are allowable over the combination of the cited references.

Claims 29 and 34 recite similar features as recited for claim 5, and thus claims 29 and 34 should be allowable for at least similar reasons as claim 5.

III. Claims 20-24, 32, 37

Claim 20 is allowable over Shoup and Schneier, alone or in combination, as those references fail to disclose or suggest all the elements of claim 20. For example, claim 20 recites "*encrypting the secret so as to generate an encrypted secret; deleting the secret; and performing a forward k out of n secret sharing algorithm on the encrypted secret so as to generate n secret owner pieces.*" In the Office Action, the Examiner concedes that Shoup does not disclose deleting the secret, but Applicant submits that Schneier does not make up for that lack in a way that either reference would suggest a combination.

In Shoup, the described use of forward k out of n secret sharing algorithm includes the encryption step mentioned on page 5. For example, on page 8 of Shoup, the private key, which is $x_i=F(i)$, is computed as part of the secret sharing algorithm and sent to server P_i. After this step, the ciphertext is computed and sent to server P_i. Thus, the calculation of the ciphertext is done after starting the secret sharing algorithm. Of further note, the recovery algorithm shows getting the message directly back after the interpolation, i.e., there is no additional decryption step that would be required if there was a previous encryption step. Thus, the encryption step is not initially done before performing the secret sharing algorithm and therefore it would not be appropriate to combine the references.

For at least the reasons stated above, Applicants submit that claim 20 is allowable over the cited references. As claim 20 is allowable, claims 21-27 dependent therefrom are also allowable for at least that reason.

Claims 32 and 37 recite similar features as recited for claim 20, and thus claims 32 and 37 should be allowable for at least similar reasons as claim 20.

35 USC §103 Rejection, Shoup in view of Schneier and Graunke

Claims 10-19, 30-31, and 35-36 stand rejected under §103(a) as being unpatentable over Shoup further in view of Schneier and Graunke.

I. Claims 10-14, 30, 35

Claim 10 is allowable over the cited references, alone or in combination, as those references fail to disclose or suggest all the elements of claim 10. Claim 10 recites similar features as recited for claim 1, and thus claim 10 and its dependent claims 11-14 should be allowable for at least similar reasons as claim 1.

Claim 10 is allowable for additional reasons. For example, claim 10 recites a method comprising "*choosing n numbers d_1 through d_n such that $e_i d_i$ mod M equals one for $1 \leq i \leq n$*". In the Office Action, the Examiner asserts that the products of the e (e_1 ... e_n) with d (d_1 ... d_n) are the K_i of Schneier.

The $e_i d_i$ products do not correspond to the K_i of Schneier because all of Schneier's K_i appear in the same equation and are multiplied by each other and then modulo M is applied to

the product. However, each $e_i d_i$ are in a separate equation (for each i), and thus all e and d do not multiply each other. This is an important distinction for otherwise the secret could not be obtained with k secret owners, where k<n. This is because all e would be required under Schneier's condition (equation 1 on page 527).

Claim 10 also recites a method comprising "*generating and storing in computer memory a database of* $\binom{n}{k}$ *values, where each value is the product of d and a unique k of the* d_i *numbers for* $1 \le i \le n$." In the Office Action, the Examiner asserts that Graunke discloses storing such values in a database.

Although Graunke may disclose saving keys in a database, Graunke does not disclose storing values that are a product of d and a unique k of the d_i numbers for $1 \le i \le n$. In other words, the key retrieved from the database in Graunke does not depend on the user or users that sent the message, nor do the keys in Schneier.

For at least the reasons stated above, Applicants submit that claim 10 is allowable over the cited references. As claim 10 is allowable, claims 11-14 dependent therefrom are also allowable for at least that reason.

Claims 15-19, 30-31, and 35-36 recite similar features as recited for claim 10, and thus should be allowable for at least similar reasons as claim 10.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Respectfully submitted,

Dated: 9/14/05

Philip H. Albert
Reg. No. 35,819

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200 Fax: 415-576-0300
PHA:jtc
60413231 v2